

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application: Carter, et al.

Serial No.: Not yet assigned

Group No.: Not yet assigned

Filed: Herewith

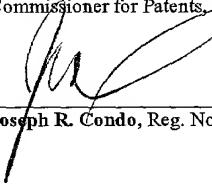
Examiner: Not yet assigned

For: ENCRYPTION AND AUTHENTICATION METHODS AND APPARATUS FOR SECURING TELEPHONE COMMUNICATIONS

"Express Mail" Label No. **EL659803508US**

Date of Deposit: **April 12, 2001**

I hereby certify that this paper is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. § 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, DC 20231.


Joseph R. Condo, Reg. No. 42,431

Assistant Commissioner for Patents
Washington, DC 20231

Sir/Madam:

PRELIMINARY AMENDMENT

Applicant respectfully requests that the Examiner amend the above-identified application as follows before examining the application.

IN THE SPECIFICATION

Please replace the paragraph beginning at page 1, line 5, with the following rewritten paragraph:

--This Application is a divisional of Application Serial No. 09/428,844, filed October 28, 1999. This application claims priority from U.S. Provisional Patent Application Serial No. 60/106,016, filed October 28, 1998, the contents of which are hereby incorporated

by reference. This application claims priority from U.S. Provisional Patent Application Serial No. 60/122,682, filed March 3, 1999, the contents of which are hereby incorporated by reference. The subject matter disclosed herein is related to the subject matter disclosed on copending application Serial No. 09/428,845, filed on October 28, 1998, entitled "Apparatus and methods for cryptographic synchronization in packet based communications."--

IN THE CLAIMS

Please cancel claims 1-18.

Please amend the claims as follows:

19. (Once Amended) An encryption device for a telephone having a handset and a base unit, the encryption device comprising:

a handset interface coupled to the handset;

a processor coupled to the handset interface having a memory for storing a set of security parameters, each said security parameter having at least one selection; and

a host interface coupled to the processor and the base unit,

wherein the processor transmits to the far-end telephone via the host interface, a message containing a representation of the set of security parameters, receives from the far-end telephone via the host interface a message containing a representation of a respective selection of each of the security parameters, and establishes a secure session with the far-end telephone based on the respective selections.

Please add the following new claims:

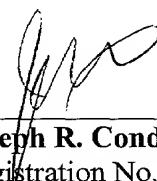
21. (New) The encryption device of claim 19, wherein the processor transmits to the far-end telephone a message containing a security mode word having a plurality of bit fields, each said bit field being associated with a respective security parameter and having a value that indicates whether the encryption device supports a corresponding selection of the associated security parameter.
22. (New) The encryption device of claim 19, wherein the set of security parameters includes a set of encryption algorithms that the encryption device supports.
23. (New) The encryption device of claim 19, wherein the set of security parameters includes a set of coding algorithms that the encryption device supports.
24. (New) The encryption device of claim 19, wherein the set of security parameters includes a set of public key modulus sizes that the encryption device supports.
25. (New) The encryption device of claim 19, wherein the set of security parameters includes a set of public key modulus sources that the encryption device supports.
26. (New) The encryption device of claim 19, wherein the set of security parameters includes a set of encryption key lengths that the encryption device supports.
27. (New) The encryption device of claim 19, wherein the respective selections represent selections of the security parameters that the far-end telephone supports.

28. (New) The encryption device of claim 28, wherein the respective selections represent the highest integrity security mode that the far-end telephone supports.

29. (New) The encryption device of claim 20, wherein the compatible parameter provides the highest integrity security mode that the encryption device supports.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendment. The attached page is captioned "Version with markings to show changes made."

Respectfully Submitted,



Joseph R. Condo
Registration No.: 42,431

Date: April 12, 2001

WOODCOCK WASHBURN KURTZ
MACKIEWICZ & NORRIS LLP
One Liberty Place - 46th Floor
Philadelphia, PA 19103
(215) 568-3100

**VERSION WITH MARKINGS TO SHOW CHANGES MADE
IN THE SPECIFICATION**

Paragraph beginning at page 1, line 5 has been amended as follows:

This Application is a divisional of Application Serial No. 09/428,844, filed
October 28, 1999. This application claims priority from U.S. Provisional Patent Application
Serial No. 60/106,016, filed October 28, 1998, the contents of which are hereby incorporated
by reference. This application claims priority from U.S. Provisional Patent Application
Serial No. 60/122,682, filed March 3, 1999, the contents of which are hereby incorporated by
reference. The subject matter disclosed herein is related to the subject matter disclosed on
copending application Serial No. [__ (attorney docket LCOM-0478)] 09/428,845, filed on
[even date herewith] October 28, 1998, entitled "Apparatus and methods for cryptographic
synchronization in packet based communications."

IN THE CLAIMS

Please cancel claims 1-18.

Please amend the claims as follows:

19. (Once Amended) An encryption device for a telephone having a handset and a base unit,
the encryption device comprising:
 a handset interface coupled to the handset;
 a processor coupled to the handset interface having a memory for storing a set
 of security parameters, each said security parameter having at least one selection; and
 a host interface coupled to the processor and the base unit,

wherein the processor transmits to the far-end telephone via the host interface, a message containing a representation of the set of security parameters, receives from the far-end telephone via the host interface a message containing a representation of a respective selection of each of the [selected security parameter selected from the set of] security parameters, and establishes a secure session with the far-end telephone based on the respective selections [selected security parameter].

Please add the following new claims:

21. (New) The encryption device of claim 19, wherein the processor transmits to the far-end telephone a message containing a security mode word having a plurality of bit fields, each said bit field being associated with a respective security parameter and having a value that indicates whether the encryption device supports a corresponding selection of the associated security parameter.
22. (New) The encryption device of claim 19, wherein the set of security parameters includes a set of encryption algorithms that the encryption device supports.
23. (New) The encryption device of claim 19, wherein the set of security parameters includes a set of coding algorithms that the encryption device supports.
24. (New) The encryption device of claim 19, wherein the set of security parameters includes a set of public key modulus sizes that the encryption device supports.
25. (New) The encryption device of claim 19, wherein the set of security parameters includes a set of public key modulus sources that the encryption device supports.

26. (New) The encryption device of claim 19, wherein the set of security parameters includes a set of encryption key lengths that the encryption device supports.
27. (New) The encryption device of claim 19, wherein the respective selections represent selections of the security parameters that the far-end telephone supports.
28. (New) The encryption device of claim 28, wherein the respective selections represent the highest integrity security mode that the far-end telephone supports.
29. (New) The encryption device of claim 20, wherein the compatible parameter provides the highest integrity security mode that the encryption device supports.